Miracle Yosua Kairupan
085155018567 | ekelcool08@gmail.com | JL. Tebet Timur III E NO.9 | www.linkedin.com/in/miracle-yosua-kairupan | miracleyk.com

Motivated university student and current IT intern at Amaan Solutions, with hands-on experience in Wazuh Server management, log analysis, and system security. Proficient in Linux system administration, penetration testing (pentest), and virtual machines (VMs) for testing and deployment. Has contributed to cybersecurity tool sales by creating product documentation and has participated in banking security discussions. Passionate about cybersecurity, ethical hacking, and system administration, seeking opportunities to further develop technical skills and contribute to real-world security solutions.

EDUCATION

BINUS University – **Kebon Jeruk** Feb 2022 – Present

Cyber Security, 3.09/4.00

- Active member of Cyber Security Community
- On-going thesis project “UTILIZING DEEP LEARNING FOR MALWARE DETECTION IN ENCRYPTED NETWORK TRAFFIC SSL OR TLS"

EXPERIENCE

PT Amaan Life Solutions – Jakarta Jan 2025 – present

IT Intern

- Assisting in Wazuh Server configuration, agent deployment, and security log analysis.
- Contribute penetration testing (pentest) assessments to identify system vulnerabilities.
- Monitoring and investigating security alerts to detect potential threats.
- Contributed to cybersecurity tool sales by creating technical documentation.
- Attended meetings on banking security issues.
- Working with Linux-based systems and configuring security tools.
- Using virtual machines (VMs) for testing and development.

PROJECT

Network Penetration Testing Write up from hack the box

- Cicada

  I gained access to the system, discovered critical credential information, and ultimately achieved full administrative access. This project demonstrated my ability to perform thorough and effective security testing.
- Cozy Hosting

  In this project, I conducted a penetration test on Cozy Hosting, identifying vulnerabilities through techniques like session hijacking, command injection, and password cracking.
- Green Horn

  I successfully exploited an RCE vulnerability in Pluck CMS (CVE-2018-1002001) on GreenHorn. By uploading a reverse shell, I gained access, escalated to the "junior" user, retrieved flags, and decoded a password to achieve root access.

System Security Scenario Projects

- Make a PHP-based dummy website that I host on my windows machine.
- Host a Wazuh manager in Ubuntu.
- Deploying the Wazuh-Agent in the windows machine.
- Used Kali Linux as an attack device to simulate real-world threats.
- Monitored and analyzed security events through Wazuh SIEM.

SKILLS

- Cybersecurity: Wazuh SIEM, Log Monitoring, Threat Detection, Penetration Testing (Pentest)
- System Administration: Linux (Ubuntu), Windows Server, Virtual Machines (VMware, VirtualBox)
- Ethical Hacking Tools: Nmap, Metasploit, Burp Suite, Wireshark
- Technical Documentation: Cybersecurity Product Documentation, Report Writing
- Programming: PHP, Python, Bash Scripting, C
- Web Development: HTML, CSS, JavaScript
- Database Management: MySQL
- Version Control: Git, GitHub